

WHAT IS CLAIMED IS:

- 1 1. A method for securing a plaintext object within a content receiver,
2 the method comprising steps of:
 - 3 receiving a secure portion of a secure object;
 - 4 receiving a plaintext remainder of the secure object;
 - 5 determining which portion of the secure object is the secure portion;
 - 6 decrypting the secure portion to provide a plaintext portion;
 - 7 forming the plaintext object that comprises the plaintext portion and the
8 plaintext remainder; and
 - 9 storing the plaintext object.
- 1 2. The method for securing the plaintext object within the content
2 receiver as recited in claim 1, further comprising steps of:
 - 3 selecting a secure portion of the plaintext object to encrypt;
 - 4 encrypting the secure portion;
 - 5 sending the secure portion and a plaintext remainder to a content receiver;
 - 6 and
 - 7 providing a key that is used in decryption of the secure portion.
- 1 3. The method for securing the plaintext object within the content
2 receiver as recited in claim 1, further comprising a step of reporting purchase of the
3 plaintext object a point away from the content receiver.
- 1 4. The method for securing the plaintext object within the content
2 receiver as recited in claim 3, wherein the second listed receiving step is performed
3 before the reporting step.
- 1 5. The method for securing the plaintext object within the content
2 receiver as recited in claim 1, wherein the decrypting step comprises a step of decrypting
3 the secure portion with an access control processor.
- 1 6. The method for securing the plaintext object within the content
2 receiver as recited in claim 1, wherein the secure portion is less than one-half the size of
3 the secure object.

1 7. A method for securing a plaintext object within a conditional
2 access system, the method comprising steps of:

3 selecting a secure portion of the plaintext object to encrypt;
4 encrypting the secure portion;
5 sending the secure portion of the plaintext object to a content receiver;
6 sending a plaintext remainder of the plaintext object to the content
7 receiver; and

8 providing a key to the content receiver wherein the key is used in
9 decryption of the secure portion.

1 8. The method for securing the plaintext object within the conditional
2 access system as recited in claim 7, further comprising steps of:

3 receiving the secure portion of a secure object;
4 receiving the plaintext remainder of the secure object;
5 determining which portion of the secure object is the secure portion;
6 decrypting the secure portion to provide a plaintext portion;
7 forming the plaintext object that comprises the plaintext portion and the
8 plaintext remainder; and
9 storing the plaintext object.

1 9. The method for securing the plaintext object within the conditional
2 access system as recited in claim 7, further comprising a step of reporting purchase of the
3 plaintext object a point away from the content receiver.

1 10. The method for securing the plaintext object within the conditional
2 access system as recited in claim 9, wherein the reporting step is performed before the
3 second listed sending step.

1 11. The method for securing the plaintext object within the conditional
2 access system as recited in claim 7, further comprising a step of determining the secure
3 portion wherein removal of the secure portion from the plaintext object renders the
4 plaintext object inoperable.

1 12. The method for securing the plaintext object within the conditional
2 access system as recited in claim 7, further comprising a step of changing authorization of
3 the content receiver from a point remote to the content receiver.

1 13. The method for securing the plaintext object within the conditional
2 access system as recited in claim 7, further comprising a step of receiving purchase
3 information from the content receiver at a location remote to the content receiver.

1 14. The method for securing the plaintext object within the conditional
2 access system as recited in claim 7, wherein the key is a symmetric key.

1 15. A method for securing an object within a content receiver, the
2 method comprising steps of:

3 receiving a first portion of the object;
4 recognizing a purchase request from a user of the content receiver for the
5 object;
6 reporting the purchase request to a point away from the content receiver;
7 receiving a second portion of the object after the reporting step; and
8 storing the object in the content receiver.

1 16. The method for securing the object within the content receiver as
2 recited in claim 15, wherein the second portion is received in encrypted form.

1 17. The method for securing the object within the content receiver as
2 recited in claim 15, wherein the first portion is greater than nine hundred percent larger
3 than the second portion.

1 18. The method for securing the object within the content receiver as
2 recited in claim 15, further comprising the step of reformulating the object from the first
3 and second portions.

1 19. The method for securing the object within the content receiver as
2 recited in claim 15, wherein the second listed receiving step comprises a step of receiving
3 the second portion by way of a secured distribution channel.